Security Policies & Procedures

This section contains security policies for the Dept.of Military Veterans Affairs.

The following documents are included in this section:

Acceptable Use Statement
For
Dept. of Military and Veterans Affairs Computing Resources

The following document outlines guidelines for use of the computing systems and facilities located at or operated by Dept. of Military and Veterans Affairs (DMAVA). The definition of DMAVA computing facilities will include any computer, server or network provided or supported by the DMAVA Network Control Center (DMAVA-NCC). Use of the computer facilities includes the use of data/programs stored on DMAVA computing systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the DMAVA-NCC. The purpose of these guidelines is to ensure that all DMAVA users (support personnel and management) use the DMAVA computing facilities in an effective, efficient, ethical and lawful manner.

DMAVA accounts are to be used only for the purpose for which they are authorized and are not to be used for non-DMAVA related activities. Unauthorized use of a DMAVA account/system is in violation of AR380-19 Information System Security and 18 U.S.C. Sec. 799 and constitutes theft and is punishable by law. Therefore, unauthorized use of DMAVA computing systems and facilities may constitute grounds for either civil or criminal prosecution.

1. The DMAVA computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a DMAVA computing system (unless secured under conditions adequate to prevent access by unauthorized persons). Information is considered “classified” if it is Top Secret, Secret and/or Confidential information, which requires safeguarding in the interest of National Security.

2. Users are responsible for protecting any information used and/or stored on/in their DMAVA accounts. Consult the Reserve Component Automation System (RCAS) User Security Guide for guidelines on protecting your account and information using the standard system protection mechanisms http://ssc-web-svr/.

3. Users are requested to report any weaknesses in DMAVA computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by DMAVA, DCSIM Help Desk or by sending electronic mail to John.DeSeignora@nj.ngb.army.mil.

4. Users shall not attempt to access any data or programs contained on DMAVA systems for which they do not have authorization or explicit consent of the owner of the data/program, the DMAVA Division Chief or the DMAVA Information System Security Manager/Officer (ISSM/ISSO).

5. Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

6. Users shall not share their DMAVA account(s) with anyone.

7. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

8. Users shall not make copies of system configuration files (e.g. /etc/passwd) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.

9. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized DMAVA user access to a DMAVA resource; obtain extra resources, beyond those allocated; circumvent DMAVA computer security measures or gain access to a DMAVA system for which proper authorization has not been given.

Electronic communication facilities (such as Email) are for authorized government use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on DMAVA systems.

Users shall not download, install or run security programs or utilities, which reveal weaknesses in the security of a system. For example, DMAVA users shall not run password-cracking programs on DMAVA Systems Division computing systems.

Users shall not access any pornographic websites or download any pornographic material.

DMAVA computing systems will not be used at any time to further personal gain.

All workstations must be powered off at the end of each business day (exceptions will be made on a case by case basis).

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the DMAVA user and the DMAVA ISSM/ISSO and can result in short-term or permanent loss of access to DMAVA computing systems. Serious violations may result in civil or criminal prosecution and other adverse actions.

I have read and understand this Acceptable Use Statement for use of the DMAVA computing systems and facility and agree to abide by it.

Signature: _____ Date: _____

Dept. of Military Veterans Affairs Special Access Policy

This policy provides a set of requirements for the regulation and use of special access on Dept. of Military Veterans Affairs (DMAVA) systems. This policy will provide a mechanism for the addition and removal of people from the special access database and a mechanism for periodic reviews of the special access database. The special access account which are covered in this policy include (some generic accounts) The documents to be included, as part of this policy are the Special Access Request form and the Special Access Guidelines agreement.

A. Policy for Regulation of Special Access Accounts:
1. Special access on DMAVA systems is maintained and monitored, via the Special Access database, by both DMAVA Operations and the DMAVA Information System Security Manager (ISSM) and/or assistant (ISSO).
2. Passwords for special access accounts are changed on a regular basis, as determined by DMAVA ISSM and/or the DMAVA System Administrator (SA).
3. Individuals authorized to receive special access passwords are required to pick up and sign for said passwords each time the passwords are changed.
4. Special access is only provided to individuals who need said access to perform their job.
5. Any misuse of special access privileges must be reported to the DMAVA Information System Security Officer within 24 hours.
6. Special access accounts are to be strictly limited and monitored by the DMAVA Information System Security Officer and/or the DMAVA SA. An example of a current special access account is the GuardNet account.
7. Persons requesting special access must follow all procedures outlined in section B of this document.
8. Persons who misuse their special access privilege can have said access revoked as outlined in Section D of this document.
9. Contents of the special access database are reviewed on a periodic basis as outlined in Section C of this document.
10. All persons who currently (prior to the approval of this policy) have special access are required to submit a completed Special Access Request form and a signed Special Access Guidelines agreement.

B. Policy for Acquiring Special Access:
1. All persons requesting special access must complete a Special Access Request form (see attachment 1). The instructions for completing the form are listed on the back. A separate form must be completed for each separate subsystem and/or branch signature that is needed. The appropriate people for approval signatures are also listed on the back of the form.
2. All persons requesting special access must read and sign the Special Access Guidelines Agreement (See attachment 2). This agreement discusses the dos and don'ts of using special access. Once a person signs the agreement he/she is then bound to abide by its contents. A copy of the signed agreement will be provided to the person for his/her personal records. The signed originals will become a part of the person's account/access file.
3. Any person refusing to sign the Special Access Guidelines Agreement will not be provided special access.
4. Persons with special access are to inform the DMAVA Information System Security Officer and/or DMAVA System Administrator if their special access requirements change.

C. Policy for Performing a Periodic Review of the Special Access Database:
A review of the special access database will be made on a regular basis or as determined by the DMAVA Security Officer. The review process will involve the following steps:
1. Two reports will be generated from the special access database. One report lists special access by system and access type. The second report lists the access by person (i.e., for each person, all access given to that person is listed).
2) The two reports are distributed to all Subsystem managers, for each system. Each person reviews the list (or appropriate part of) to determine if any changes should be made.
3) All persons requesting changes to the database must forward their comments to DMAVA Security Officer.
4) Should anyone determine that an individual needs to be added to other special access groups, that individual must submit a Special Access Request form requesting additional access.

5) If there are any deletions to be made to the database, the proper procedure outlined in Section D must be followed.

D. Policy for Removing People from the Special Access Database:
1. A person may be removed from the special access database for one of three reasons:
- The person no longer works at DMAVA
- The person no longer needs special access due to a change in job duties
- The person has violated the Special Access Guidelines agreement.
2. A person may be removed from the special access database at any time as determined by the DMAVA Security Officer and/or appropriate Branch Chief or during one of the regular reviews of the database as described in Section C.
3. The procedures for removing a person from the special access database are as follows:
Case One: Person no longer works at DMAVA
1. Fill out a Special Access Request form specifying the removal of all access.
2. Have DMAVA Security Officer, or his designated assistant, sign form.
3. Update database and change affected password(s) within five working days.
4. Notify appropriate Branch Chief about deletion(s).

Case Two: Person no longer needs special access due to a change in job duties
1) Fill out Special Access Request Form specifying the removal of appropriate access(es).
2) Have employee's manager sign form. (**NOTE** This is for information only)
3) Have appropriate Subsystem Manager and/or Branch Chief sign form.
4) Update database during the next change of passwords.

Case Three: Person violated the Special Access Guidelines agreement
1) Appropriate people (i.e., Subsystem manager, DMAVA Security Officer, Branch Chief) must decide if the violation constitutes removal of all special access of that person or just the special access involved.
2) Fill out Special Access Request Form specifying removal of appropriate access.
3) Have employee's manager sign form.
4) Have appropriate Subsystem Manager and Branch Chief sign form.
5) Update database and change passwords within 24 hours.

Approved by: _____ Concurrence: _____

Dept. of Military Veterans Affairs Special Access Guidelines Agreement

This agreement outlines the many do's and don'ts of using special access on Dept. of Military Veterans Affairs (DMAVA) computers. Special access is defined as having the privilege and password to use one or more of the following accounts: (GuardNet, Network Folders/Drives). The DMAVA environment is very complex and dynamic. Due to the number and variety of computers and peripherals, special access must be granted to numerous people so the DMAVA facility can be properly supported. People with special access must develop the proper skill for using that access responsibly.
The Special Access Guidelines have been developed to help people to use their special access in a responsible and secure manner. All persons requesting special access must read and sign this agreement. Anyone refusing to sign this agreement will not be granted the special access that they requested.

General Guidelines
1. Be aware of the DMAVA environment. The DMAVA facility is a highly specialized facility containing a large number of computers of different configurations. Many daily system tasks have been automated by the use of software tools. Be aware of the DMAVA Way" of doing system tasks.
2. Always log on systems where you have an account as yourself. Any action done under a special access account should have an audit trail.
3. Use special access only if necessary. Many system tasks require the use of root, admin or other special access. However, there are many tasks that can be done without the use of special access. When at all possible use regular accounts for trouble-shooting and investigating.
4. Document all major actions and/or inform appropriate people. Documentation provides a method to analyze what happened. In the future, others may want to know what was done to correct a certain problem. The System Administrator or Network Administrator is to be informed BEFORE any changes are made to system specific or configuration files.
5. Have a backup plan in case something goes wrong. Special access, especially root, admin has a large potential for doing damage with just a few keystrokes. Develop a backup plan in case something goes wrong. You must be able to restore the system to its state before the error occurred.
6. Know whom to turn to if problems arise. With the use of special access, situations arise that have never come up before. Although DMAVA has many written procedures, they do not cover every circumstance possible. If any doubt exists about how you should proceed on a problem, then ask for assistance. Know whom to ask.

Specific Do not's of Special Access
1. Do not share special access passwords with anyone.
2. Do not write down the special access passwords or the current algorithm.
3. Do not routinely log onto a system, for which you have an account, as "root, admin" or any other special access account.
4. Do not read or send personal mail, play games, read the net news or edit personal files using a special access account.
5. Do not browse other user's files, directories or E-mail using a special access account.
6. Do not make a change on any system that is not directly related to your job duties. The System Administration is responsible for approving all changes to the systems(s) of his/her responsibility. No changes are to be made to any system configuration file or executable file with prior approval of the "System Administrator". Making a change AND then informing the SA is considered a violation of this guideline.
7. Do not use special access to create temporary files or directories for your own personal use.

I certify that I have read the above guidelines and will use this special access in accordance with DMAVA guidelines and policies. Misuse of any special access privilege will result in removal of that access.

Signature: _____ Date: _____

Dept. of Military and Veterans Affairs Escalation Procedures for Security Incidents

This procedure describes the steps, which are to be taken for physical, and computer security incidents, which occur within the facility of the work place. The type of incidents has been classified into three levels depending on severity. The Level One incidents are least severe and should be handled within one working day after the event occurs. Level Two incidents are more serious and should be handled the same day the event occurs (usually within two to fours hours of the event). Level Three incidents are the most serious and should be handled as soon as possible. For additional information on incident response and handling refer to the "DMAVA Security Incident Handling Procedures."

List of Contacts

Computer Security Incidents:
1) Loss of Personal Password Sheet (Level One Incident)
A. Notify the NCC (Network Control Center), Information System Security Manager/Officer (ISSM/ISSO) or Dept. of Military & Veterans Affairs (DMAVA) Help Desk within one working day.
B. The ISSM/ISSO will decide if a password change is necessary.

2) Suspected Sharing of Accounts (Level One Incident)
A. Users will document all pertinent information on a NCC report.
B. The ISSM/ISSO or NCC will call person(s) suspected of account sharing and determine severeness of the incident. In most cases, people who share accounts have a valid need to have their own accounts. In these cases, the user(s) account will remain disabled until account request forms are received and process the person who was using the user(s) account.
C. The NCC will escalate the issue to higher management if necessary.

3) Employee Termination Due to Adverse Action (Level Two Incident)
A. Notify ISSM/ISSO and NCC within two hours. If neither can be reached within two hours, contact the (DMAVA) Help Desk.
B. Upon request from NCC or ISSM/ISSO, all accounts for a terminated employee will disable. At this point, members of Emergency Operation Center (EOC) team are not permitted to provide access (building or otherwise) to the terminated employee.
D. EOC will ensure building access is disabled and will confiscate card key, if possible.
E. The NCC or ISSM/ISSO will change systems passwords.
F. If necessary, the ISSM/ISSO will escalate issue to DMAVA Division Office.

4) Suspected Violation of Special Access (Level Two Incident)
The misuse of Special Access is defined in the document "Special Access Guidelines Agreement" which is signed by each person having Special Access at NCC.
Minor Violations - No threat to Network Security
A. Notify NCC within one working day. If unable to reach NCC within that time, contact the ISSM/ISSO or the DMAVA Help Desk. You should also inform the manager of the person suspected of violating the policy.
B. The NCC, ISSM/ISSO will determine who is involved in the violation and the extent of the violation.
C. Notify the ISSM /ISSO within two working days.
D. If necessary, the NCC, ISSM/ISSO will escalate issue to Deputy Chief of Staff for Information Management Office (DCSIM).
Major Violations - Possible threat to Network Security
A. Notify NCC within one hour. If cannot be reached within two hours, contact the DMAVA Help Desk.
B. Notify ISSM/ISSO within four hours. If he can not be reached within that time, contact his DMAVA Help Desk.
C. Disable all accounts for involved people.
D. Begin process of changing all system passwords.
E. Take further action as deemed necessary by NCC.
5) Suspected Computer Break-in or Computer Virus (Level Three Incident)
A. Isolate infected systems from the remaining network as soon as possible. The NCC staff should consult the LAN/WAN teams to determine the best method to isolate the infected systems from the remaining network.

B. If a computer virus/worm is suspected, isolate network from outside networks as soon as possible. The LAN and WAN teams should be consulted before the disconnect takes place to discuss the best method and feasibility for doing a full disconnect from the Internet.
C. Notify NCC as soon as possible. If unable to reach him/her within ten minutes, contact the DMAVA Help Desk.
D. Notify ISSM/ISSO within one hour. ISSM/ISSO will escalate to higher level management if necessary.
E. Notify all involved DCSIM's within two hours.
F. While waiting for DCSIM to respond, attempt to trace origin of attack and determine how many systems (if any) have been compromised. Save copies of system log files and any other files, which may be pertinent to incident.
G. DCSIM will decide what further actions are needed and assign appropriate people to perform the tasks.
H. Upon completion of the investigation, the NCC, ISSM/ISSO will write an incident summary report and submit to the appropriate levels of management.

Physical Security Incidents:
1) Unauthorized Building Access (Level Two Incident)
If during regular working hours an unauthorized person is in the building or in a controlled area, call or page the ISSM/ISSO or EOC immediately. If after working hours, call voice mail and it will page appropriate person ISSM/ISSO or EOC.
B. Escort the person outside the building or controlled area. Log incident and report to ISSM/ISSO.
C. The ISSM/ISSO or EOC will decide upon the appropriate action to take
2) Property Destruction or Personal Theft (Level Two or Three Incident)
A. Unless the theft or destruction is major, notifies the ISSM/ISSO and NCC within one working day. If unable to reach ISSM/ISSO within one working day, contact the Help Desk. Otherwise, for major theft or property destruction, notify ISSM/ISSO immediately. If he/she can not be reached within one hour, call or page ISSM/ISSO through voice mails.
B. If destruction involves a NCC computer, notify within 24 hours.
C. If incident involves theft of NCC property, contact the DMAVA-NCC within two working days. The NCC will contact the Property Custodian, if necessary.
D. The ISSM/ISSO will escalate incident to DCSIM Office as necessary.

Dept. of Military Veterans Affairs Incident Handling Procedure

1.0 INTRODUCTION

This document provides some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide Dept. of Military Veterans Affairs (DMAVA) support personnel with some guidelines on what to do if they discover a security incident. The term incident in this document is defined as any irregular or adverse event that occurs on any part of the Network. Some examples of possible incident categories include compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

* You see a strange process running and accumulating a lot of CPU time.
* You have discovered an intruder logged into your system.
* You have discovered a virus has infected your system.
* You have determined that someone from a remote site is trying to penetrate the system.

The steps involved in handling a security incident are categorized into five stages: protection of the system; identification of the problem; containment of the problem; eradication of the problem; recovering from the incident and the follow-up analysis. The actions taken in some of these stages are common to all types of security incidents and are discussed in section 2. Section 3 discusses specific procedures for dealing with worm/virus incidents and hacker/cracker incidents.

1.1 TERMS

Some terms used in this document are:

ISSM – Information System Security Manager
ISSO – Information System Security Officer
SA – System Administrator
CERT - Computer Emergency Response Team

1.2 AREAS OF RESPONSIBILITY

In many cases, a single person on a single system will not perform the actions outlined in this guideline. Many people may be involved during the course of an active security incident, which affects several of the DMAVA systems at one time (i.e., a worm attack). The DMAVA should always be involved in the investigation of any security incident.

The DMAVA ISSM SSG DeSeignora, the DMAVA ISSO 1LT. Bobinis and the /DMAVA SA CW2 Sleeper and SGT Achenbach will act as the incident coordination team for all security-related incidents. In minor incidents, only the DMAVA SA will be involved. However, in more severe incidents all three may be involved in the coordination effort. The incident coordination team will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and clean up are responsible for providing any needed information to members of the incident coordination team.

Any directives given by a member of the incident coordination team will supersede this document.

1.3 IMPORTANT CONSIDERATIONS

A computer security incident can occur at anytime of the day or night. Although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be watching their flocks. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident. Providing information to the wrong people could have undesirable side effects. Section 2.3 discusses the policy on release of information.

2.0 GENERAL PROCEDURES

This section discusses procedures that are common for all types of security incidents.

2.1 KEEP A LOG BOOK

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under

investigation. The information should be logged in a location that can not be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

* Dates and times of incident-related phone calls.
* Dates and times when incident-related events were discovered or occurred.
* Amount of time spent working on incident-related tasks.
* People you have contacted or have contacted you.
* Names of systems, programs or networks that have been affected.

2.2 INFORM THE APPROPRIATE PEOPLE

Informing the appropriate people is of extreme importance. There are some actions that can only be authorized by the DMAVA-ISSM/ISSO or /DMAVA- SA's. DMAVA also has the responsibility to inform other sites about an incident, which may effect them. A list of contacts is provided below. Section 3 discusses who should be called and when for each type of security incident.
Phone numbers for the people below can be obtained from the DMAVA -Help Desk.

List of Contacts
DMAVA-ISSM –John Z DeSeignora (609) 530-6923, DSN 445-9923

DMAVA-ISSO – Michael A Bobinis (609) 530-6936, DSN 445-9936

DMAVA-NCC SA – Paul H Sleeper (609) 530-7159, DSN 445-9159

DMAVA-NCC SA – Pete Achenbach (609) 530-7163, DSN 4459163

DMAVA-Help Desk –(609) 530-6899, DSN 445-9899

2.3 RELEASE OF INFORMATION

Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. All release of information must be authorized by the DMAVA -ISSM or by other people designated by the DMAVA-ISSM. All requests for press releases must be forwarded to the Branch or Division level. Also, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be a security officer from another site. All suspicious requests for information (i.e., requests made by callers claiming to be a DMAVA-SA for another site) should be forwarded to the DMAVA-ISSM or Branch level. If there is any doubt about whether you can release a specific piece of information contact the DMAVA-ISSO or DMAVA-SA.

2.4 FOLLOW-UP ANALYSIS

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., and should be removed from the system(s). If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by theDMAVA -ISSM/ISSO and distributed to all appropriate personnel.

3.0 INCIDENT SPECIFIC PROCEDURES

This section discusses the procedure for handling virus, worm and hacker/cracker incidents.

3.1 VIRUS AND WORM INCIDENTS

Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes; thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, then proceed as if the attack was worm related.

3.1.1 Isolate the System

Isolate infected system(s) from the remaining DMAVA network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the DMAVA from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since DMAVA will be disconnected from sites, which may have patches. The DMAVA -ISSM/ISSO must authorize the isolation of the DMAVA network from the outside world. Log all actions.

Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.

3.1.2 Notify Appropriate People

Notify the DMAVA SA as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. DMAVA SA will then be responsible for notifying other appropriate personnel. *** NOTE - Below, different times are given for suspected worm attack and for a suspected virus attack.

- The DMAVA SA will notify the DMAVA -ISSO as soon as possible. If unable to reach him within one hour (10 minutes for a worm attack), his backup person will be contacted.
- The DMAVA SA will notify the DCSIM-ISSO within two hours (one hour for a worm attack). The DMAVA -ISSO will escalate to higher level management if necessary.
- The DMAVA SA should notify all involved SAs within four hours (two hours for a worm attack).

3.1.3 Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Below is a list of tasks to make a snapshot of the system:

1) Save a copy of all system log files. The log files are usually located in /usr/adm.
2) Save a copy of the root history file, */.history*.
3) Save copies of the */etc/utmp* and */etc/wtmp* files. Sometimes these files are found in the */usr/adm* directory.
4). Capture all process status information in a file using the command ps -awwxl > file name for BSD systems and ps -efl > file name for SYSV systems.

If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snapshot information on the system.

Run scan disk on the infected system(s) to identify other possible problems such as altered system files, new suid programs or hidden special files.

If other sites have been involved at this point, they may have helpful information on the problem and possible short-term solutions. Also, any helpful information gained about the virus or worm should be passed along to CERT sites, after approval by DMAVA - ISSO. Log all actions.

3.1.4 Contain the virus or worm

All suspicious processes should now be halted and removed from the system. Make a full dump of the system and store in a safe place. The tapes should be carefully labeled so unsuspecting people will not use them in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all DMAVA systems have been inoculated and/or the other Internet sites have been cleaned up and inoculated. Log all actions.

3.1.5 Inoculate the System(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the tasks of assessing the damage are not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. Log all actions.

3.1.6 Return to a Normal Operating Mode

Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. Log all actions.

3.1.7 Follow-up Analysis

Perform follow-up analysis as described section 2.4.

3.2. HACKER/CRACKER INCIDENTS

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to the DMAVA NETWORK.

Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events, which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible.

There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state (see section 3.2.2). The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to a identification and possible criminal conviction (see section 3.2.3). The level of understanding of the risks involved will determine the method used to handle a cracker/hacker incident.

3.2.1 Attempted Probes into a DMAVA System

Incidents of this type would include repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts.

3.2.1.1 Identify Problem

Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Log all actions.

3.2.1.2 Notify DMAVA -ISSM

Notify the DMAVA -ISSM within 30 minutes. If the DMAVA -ISSM can not be reached then notify the DMAVA -ISSO or the DMAVA SA or DMAVA -Help Desk. The DMAVA - SA or Help Disk will be responsible for notifying other levels of management.

3.2.1.3 Identify Hacker/Cracker

If the source of the attacks can be identified, then the DMAVA SA (or a designated person) will contact the system administrator or ISSO for that site and attempt to obtain the identify of the hacker/cracker. If the hacker/cracker can be identified, the information should be provided to the DMAVA -ISSM or ISSO. The DMAVA -ISSM or ISSO will provide directions on how to proceed, if necessary. Log all actions.

3.2.1.4 Notify CERT

If the source of the attacks can not be identified, then the DMAVA -ISSM/ISSO or SA will contact the CERT teams and provide them with information concerning the attack. ***NOTE - the DMAVA team or someone he designates must approve Release of information. Log all actions.

3.2.1.5 Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the DMAVA SA or DMAVA -ISSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

3.2.2 Active Hacker/Cracker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. The DMAVA-ISSM/ISSO or someone he designates (i.e., the DMAVA SA) must make this decision. The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

3.2.2.1 Notify Appropriate People

Notify the DMAVA SA as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The DMAVA -ISSO will then be responsible for notifying other appropriate personnel. The DMAVA SA, with possible help from the involved SA, will be responsible for trying to assess what the hacker/cracker is after and the risks involved in letting the hacker/cracker continue his/her activity.

The DMAVA -ISSO will notify the DMAVA -ISSM as soon as possible. If unable to reach him within ten minutes, his backup person should be contacted. The DMAVA -ISSO can make the decision to allow the hacker to continue or to lock him out of the system. Based on the decision, follow the procedures in 3.2.3.1 or 3.2.3.2 below.
The DMAVA SA or DMAVA -ISSO will notify the DMAVA -ISSM within 30 minutes. The /DMAVA -ISSM will escalate to higher level management if necessary.

3.2.3 Removal of Hacker/Cracker from the System
3.2.3.1 Snap-shot the System
Make copies of all audit trail information such as system logs files, the root history files, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snapshot information on the system. Log all actions.
3.2.3.2 Lock Out the Hacker
Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. Log all actions.
3.2.3.3 Restore the System
Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the logbook for this incident. Log all actions.
3.2.3.4 Notify Other Agencies
Report the incident to the ACERT, RCERT and to MACON. ***NOTE- Release of information must be approved by the DMAVA -ISSM or someone he designates. Log all actions.
3.2.3.5 Follow-up
After the investigation, a short report describing the incident and actions that were taken should be written by the DMAVA -NCC SA or DMAVA -ISSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.
3.2.4 Monitoring of Hacker/Cracker Activity
There are no set procedures for monitoring the activity of a hacker. Each incident will be dealt with on a case by case basis. The DMAVA -ISSM or the person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system(s), the steps outlined in section 3.2.3 above should be followed.
3.2.5 Evidence of Past Incidents
In the case of where an incident is discovered after the fact, there is not always a lot of evidence available to identify who the person was or how they gained access to the system. If you should discover that someone had successfully broke into a DMAVA system, notify the DMAVA SA within one working day. The DMAVA SA will be responsible for notifying the appropriate people and investigating the incident.

Dept. of Military & Veterans Affairs Personnel Software Policy

The New Jersey National Guard licenses the use of copies of the computer software from a variety of outside companies. The New Jersey National Guard does not own the copyright to this software or its related documentation except for a single copy for backup purposes or unless expressly authorized by the copyright owner(s), does not have the right to reproduce it for use on more than one computer. With regard to software

usage on local area networks, the New Jersey Army National Guard shall use the software only in accordance with the license agreement.

New Jersey National Guard employees are not permitted to install their own copies of any software onto New Jersey National Guard machines. New Jersey National Guard employees are not permitted to copy software from the New Jersey National Guard computers and install it on home or any other computers. Exception! Norton or McAfee anti-virus software is the only authorized software you can borrow to install on your home PC.

New Jersey National Guard employees learning of any misuse of software or related documentation within the organization shall notify Information Security Office 609-530-6923. According to the U.S. law, unauthorized reproduction of software is a federal offense. Offenders are subject to civil damages up to $100,000 per title copied, and criminal penalties, including fines (up to $250,000 per title copied) and imprisonment (up to 5 years per title copied). This applies to ALL of the parties involved, from the actual violator to the supervisor in the chain of command, to the Chief of Staff, up to the Adjutant General. Penalties up to a ten-year prison term could be levied against repeat offenders.

Any New Jersey National Guard employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the New Jersey National Guard or who places or uses unauthorized software on the New Jersey National Guard premises or equipment shall be subject to disciplinary action. The New Jersey National Guard does not condone and specifically forbids the unauthorized duplication of software.

All employees issued computers owned by the New Jersey National Guard will be provided a written copy of this software policy. All computer users will be asked to sign a separate statement certifying knowledge of, and agreement with, New Jersey National Guard software policy.

Detailed Software Policy Provisions

Everyone in the New Jersey National Guard Benefits from a healthy computer software industry.

In the workplace, “piracy” is characterized by two common incidents: extra copies of software are made for employees to take home, and extra copies are made for the office. Both situations mean a greater number of computers can run more copies of the software than were originally purchased. Both situations are a crime.

Unless a special arrangement has been made between the user and the publisher, the user must follow a simple rule: one software package per computer. This means that a copy of software should be purchased for every computer on which it will be used. For example, if the business has 10 computers on which employees use spreadsheets software it must purchase 10 copies of such software. If there are 25 secretaries using word processing software on their computers each secretary must have a licensed copy.

Another option that has proven successful is for firms to enter into special site license or concurrent use agreements with publishers. Their agreements compensate the publishers for the “lost sales” they might have made on a package-by-package basis. With a site license, the company agrees to pay a certain amount for a specific number of copies they will make and not exceed on site. Concurrent license permits a specified number of users to access the software simultaneously, but prohibits users from exceeding the number of licenses acquired by the company and as metered by the program. These types of licenses will therefore, often save the organization money. At the same time, they eliminate the possibility that copyright violations will occur. By buying the correct number of programs or the right type of license, a company removes the incentive for employees to make unauthorized copies. Adhering to these rules will pay off in the long run, because an organization that illegally duplicates software exposes itself to tremendous liability. Supervisors that do not take reasonable and prudent measures to uncover software piracy or ignore it are subject to the same punishments as the thief making the copies.

It has been found that when companies enact a policy statement stating their intention to ensure employee compliance with copyright regulation, the risk of the software piracy is reduced.

Conclusion

Most people do not purposely break the law. They would never consider stealing a package of software from the shelf of a retail store. But those who copy software without authorization are also stealing intellectual property and they must understand the consequences of their actions.

Software Policy
Acceptance and Agreement Form

I have received a written copy of the New Jersey National Guard's Software Policy. I fully understand the terms of this policy and agree to abide by them. I realize that the New Jersey National Guard will use security software and unannounced software audits to monitor my compliance with the policy. I acknowledge that I have no presumption of privacy on New Jersey National Guard's automation equipment, regardless of its nature. I understand that violations of this policy could lead to loss of automation privileges and/or disciplinary action.

Dept. of Military and Veterans Affairs Internet Usage and Security Policy.

The New Jersey Army National Guard provides access to the vast information resources of the Internet to help you do your job faster and smarter, and be a well-informed government employee. The facilities to provide the access represent a considerable commitment of government resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand the expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While this Policy will set forth-explicit requirements for Internet usage below, I would like to start by describing our Internet usage philosophy. First and foremost, the Internet for the New Jersey Army National Guard is a business tool, provided to you at significant cost. That means I expect you to use the Internet access exclusively for business-related purpose; i.e. to communicate with other government agencies to research relevant topics and obtain useful information. Conduct yourself honestly and appropriately on the Internet, and

respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other work-related dealings. To be absolutely clear on this point, all existing NJARNG policies apply to your conduct on the Internet, especially those that deal with intellectual property protection, privacy, misuse of government resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the New Jersey Army National Guard and expose the government to significant legal liabilities.

Access to the Internet gives each individual Internet user an immense and unprecedented reach to propagate government messages and tell the National Guard story. Because of that power, we must take special care to maintain the clarity, consistency and integrity of the New Jersey Guard's corporate image and posture. Anything any one employee writes in the course of acting for the government on the Internet can be taken as representing the National Guard's corporate posture. That is why we expect you to exercise good judgment when you participate on the Internet for government business, as outlined below.

While our direct connection to the Internet offers many potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, which may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

Certain terms in this policy should be understood expansively to include related concepts. New Jersey Army National Guard includes all employees, full-time federal and state and M-Day soldiers. Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop

_____ _____

Today's Date Name: Last, First, Middle

_____

Signature

Password Control

A. User identification (user-ID) and passwords, because of their cost-efficiency and ease of implementation, are the most common identification and authentication (I&A) procedures. Because of their vulnerablitlity to interception or inadvertent disclosure, they are also the weakest of I&A methods. Passwords are only effective when used properly. Inappropriate passwords create some of todays most common information system vulnerabilities.
B. Prior to issuing passwords and user-IDs, make sure the user has taken appropriate computer security training. Make sure the user is briefed on the importance of protecting their user-ID and password; reporting any suspicious activity, fraud, waste, and abuse; and the use of system monitoring following the incident reporting process found in DA PAM 25-IA.
C. Passwords generated by the Information System (IS).
   1.) Passwords generated by the user must meet the criteria of AR 25-IA.

2.) Passwords will be at least eight alphanumeric characters (upper and lower case) with at least two numeric/special characters (1, 2. @. #. $. %. etc). Never make a password related to one's own personal identity, history, or environment.

D. Generic password assignment is prohibited (e.g. system having "welcome" as the password for all newly created accounts) unless the user is required to change the password upon initial assignment.

E. Limit the number of attempts allowed for correct password entry. Set the degree of password entry protection and the number of allowed entry attempts according to the sensitivity of the protected data. Normally three attempts are permitted.

F. When the maximum amount of password attempts are exceeded, lock out the user-ID and/or terminal from use. Make sure these procedures cannot be defeated by a user, or used to cause a denial of service by locking out all user-IDs or terminals. Make sure procedures are in place so the user must request reinstatement from the IASO/system administrator.

G. Each user is responsible and accountable for their own password.

H. Users must memorize their password. Do not place passwords on desks, walls, and sides of terminals or store them in a function key, log-in script, or the communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a safe.

I. Users must enter their identifier and password upon initial access to an information system. A user must enter a password in such a manner that the password is not revealed to anyone observing the entry process.

J. Do not share passwords for individual accounts. Passwords for group and organizational accounts may be shared when necessary for mission accomplishment. When password sharing is necessary for mission accomplishment make sure the password is changed immediately after shared access is no longer required. If an individual having access to the shared password no longer requires access, the password will be changed immediately.

K. Users may use an established procedure to change their own password whether it is machine or user generated. Passwords must never be issued over the telephone, fax or emailed. The user must enter the old password and authenticate as part of the password change procedure.

(1) If the user forgets the password, the system administrator/help desk must authenticate the user's identity before changing the password.

(2) If given a generic password (e.g. "password"), the system must prompt the user to immediately change to a new password. If the system is incapable of such a function, the IASO or system administrator must walk the user through the password change procedure.

L. Remove user-IDs and passwords from an IS whenever the user is permanently transferred to another location or terminates employment.

M. Suggestions for choosing a good password:

(1) Your password is the key to your account. It should be easy to remember, but very hard for someone else to guess.

(2) Do not use your user-ID, a name, a hobby, or a single dictionary word.

(3) Do not use your social security, telephone, or license plate numbers.

(4) Do use a mix of uppercase and lowercase letters and a special character, swim!3MileS, IgolFer*, 2FORU&me.

(5) Do misspell words or replace syllables with numbers and special characters 1onderFul!, For2natE#, aPHORDit$, 56sheVY+, bOOik4u<.

(6) Do use 2 or 3 words together Ear2Knee+, 1BignosE%, BAG4golf!, MaiL4You=.

Do use the first letter of each word in a sentence – "My three dear Daughters are very beautiful!" would become M3dDavb! And "My one son is a diligent worker!" would become M1siadw!

Rules for Passwords

The DMAVA uses robust password security. When you create a new password, the following rules apply:

1. Passwords must be at least eight (8) characters long.

2. Passwords must contain characters from at least three (3) of the following four (4) character types.

Description	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric "special characters" such as punctuation symbols	!@#$^&*()_+;-?

3. Passwords must not contain your user name or any part of your full name. Do not use the name of a relative or pet. Passwords must not contain any dictionary word or name. This is key to a good password. Do not write down the password. Take a moment to create a memory device for remembering the password.

4. The DMAVANet requires you to change your password every 180 days. It also keeps a history file of the last eight passwords you have used and will not allow you to reuse passwords. Change your password while in your home domain; changing passwords across domains does not work reliably.

5. If you receive Error 59, the most likely cause is one or more violations of the preceding criteria.

6. This will make the password easier for the user to remember, it will meet the requirements of network security, it will automate what has been a tedious and manpower intensive procedure that will allow the CIO to redirect assets to higher priority security procedures and will allow immediate changes if the user believes their password has been compromised.

When You Forget Your Password

If you forget your LAN password, you will have to call the Help Desk to have your password reset. The Help Desk (609-530-6899) will provide a temporary password to get you back into your application, where you will be prompted to establish a new private password of your choosing. In providing you with your temporary password the Help Desk will create a permanent record of the transaction in its Remedy System, and will require your DMAVA badge number, SSN or Date of Birth as proof of your identity and authorization. The badge number, SSN or Date of Birth will be checked against the DMAVA Security database to ensure authenticity.